

Amrita Vishwa Vidyapeetham



15CSE312 - Computer Networks Case Study Document Design and Simulation of VLAN

Team:

Reg. No	Name	Email	Contribution
CB.EN.U4CSE17040	Manojkumar V K	vkmanojk@gmail.com	Architecture Diagram, Cisco Packet Tracer, Implementation of Network Architecture, Sufficiency of the Network
CB.EN.U4CSE17059	Sudharshan S	sudharshanspr@gmail.com	Implementation of RIP in Python, Analytical Questions.
CB.EN.U4CSE17062	Tadi Aravind	aravind.tadi2000@gmail.com	QoS Parameters - Bandwidth, Throughput, Packet Loss, Propagation Delay.
CB.EN.U4CSE17064	Sritanvi T	sritanvithirunagari@gmail.com	Performance Parameters - TransmissionTime, ProcessingDelay, Queueing Delay, Network Latency.

Abstract:

The project is to understand the advantages of using VLAN in a network, and how broadcasting is controlled. Understand the configuration which is required to setup a vlan based network using Cisco routers and switches. The main goal of this work is to increase the security level of the LAN, in order to reduce the access of undesirable sites and to avoid the presence of hackers on the internet.

(a) Problem Statement:

The objective of the case study is to create a secure VLAN for an enterprise located at all four metropolitan cities. Each location has specific requirements:

1. Chennai: The Chennai location contains the Web Server(192.168.8.2/24) and the Mail server(192.168.8.3/24). Chennai router is configured with proper banner and enable secret as 'chennai@cisco' and VTY password as 'cisco'.
2. Kolkata: The Kolkata location has 3 VLANS. They are VLAN 10(Sales), VLAN 20(Finance) and VLAN 30(HR). The kolkata router is configured with proper banner and enable secret as 'kolkata@cisco' and VTY password as 'cisco'.
3. Delhi: The Delhi location has 2 VLANs. They are VLAN 100(WareHouse) and VLAN 200(Factory). Delhi router is configured with proper banner and enable secret as 'delhi@cisco', VTY password as 'cisco'.
4. Mumbai: The mumbai location has only the office LAN in 192.168.100.0/24 subnet and each computer is getting IP address from the DHCP Server 192.168.10.02/24. Mumbai router is configured with a proper banner. The enable secret is 'mumbai@cisco' and VTY password is 'cisco'.

All the locations are connected via P2P leased lines. Users of all regions except the Factory VLAN will have access to the WebServer and Mail server. Inter VLAN routing has been performed and RIPv2 is used as the routing protocol.

(b) Software:

- This stack includes a custom made VLAN
- Modified version of Routing Information Protocol is used.
- Cisco Packet Tracer to simulate network topologies and imitate the functioning of a network.

(c) Analytical Questions:

- What is the average Round Trip Time of the proposed network?
5 ms
- How does one prevent bottlenecks in the network, i.e., manage flow control?
The use of VLAN in the proposed architecture is an efficient mechanism to prevent bottlenecks
- When more users connect, does the network suffer ?
Although the network is affected with the increase in the number of users, the efficiency of the proposed design still would be much greater than ordinary network topology.
- How to compute the shortest route from source to destination?
In the routing algorithm, dynamic programming is used to calculate the shortest route so that the time and space complexity is minimum.
- Why is this network architecture preferable over the traditional network already present?
The use of VLANs over LANs prove to be efficient in many ways including congestion control, network security, etc.
- What is the queueing strategy followed ?
First In First Out and weighted fair
- What is the average propagation delay and bandwidth of the network ?
Propagation delay is 100 μ s and bandwidth is 10000 Kbit
- What is the size of the maximum transmission unit ?
1500 bytes

(d) Data Tables:

IP Addressing: Our proposed system uses class C addressing to accommodate the nodes present in our network. The number of nodes is confined to the IP space .i.e 254 nodes in the network

Routers: A router is a networking device that forwards data packets between computer networks. Routers perform the traffic directing functions on the Internet. Data sent through the internet, such as a web page or email, is in the form of data packets. A packet is typically forwarded from one router to another router through the networks that constitute an internetwork (e.g. the Internet) until it reaches its destination node.

Switches: A network switch (also called switching hub, bridging hub, or MAC bridge) is networking hardware that connects devices on a computer network by using packet switching to receive and forward data to the destination device.

VLAN: A virtual local area network (VLAN) is a logical group of workstations, servers and network devices that appear to be on the same LAN despite their geographical distribution. A VLAN allows a network of computers and users to communicate in a simulated environment as if they exist in a single LAN and are sharing a single broadcast and multicast domain. VLANs are implemented to achieve scalability, security and ease of network management and can quickly adapt to changes in network requirements and relocation of workstations and server nodes.

End devices: The network devices that people are most familiar with are called end devices. All computers connected to a network that participate directly in network communication are classified as hosts. These devices form the interface between users and the underlying communication network.

DHCP Servers: DHCP (Dynamic Host Configuration Protocol) server automatically sends the required network parameters for clients to properly communicate on the network. Without it, the network administrator has to manually set up every client that joins the network, which can be cumbersome, especially in large networks. DHCP servers usually assign each client with a unique dynamic IP address, which changes when the client's lease for that IP address has expired.

(e) Model Diagram of proposed Network Design:



Figure 1: Connection between cities

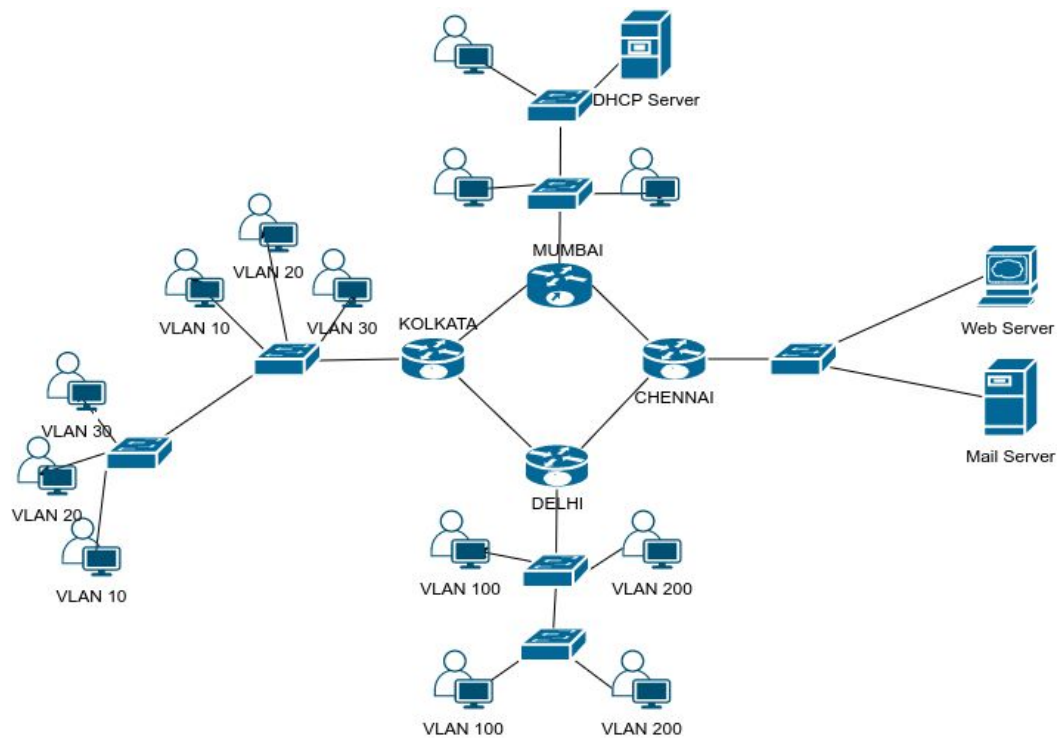


Figure 2: Proposed design of Network Topology

(f) Network Design in Cisco Packet Tracer:

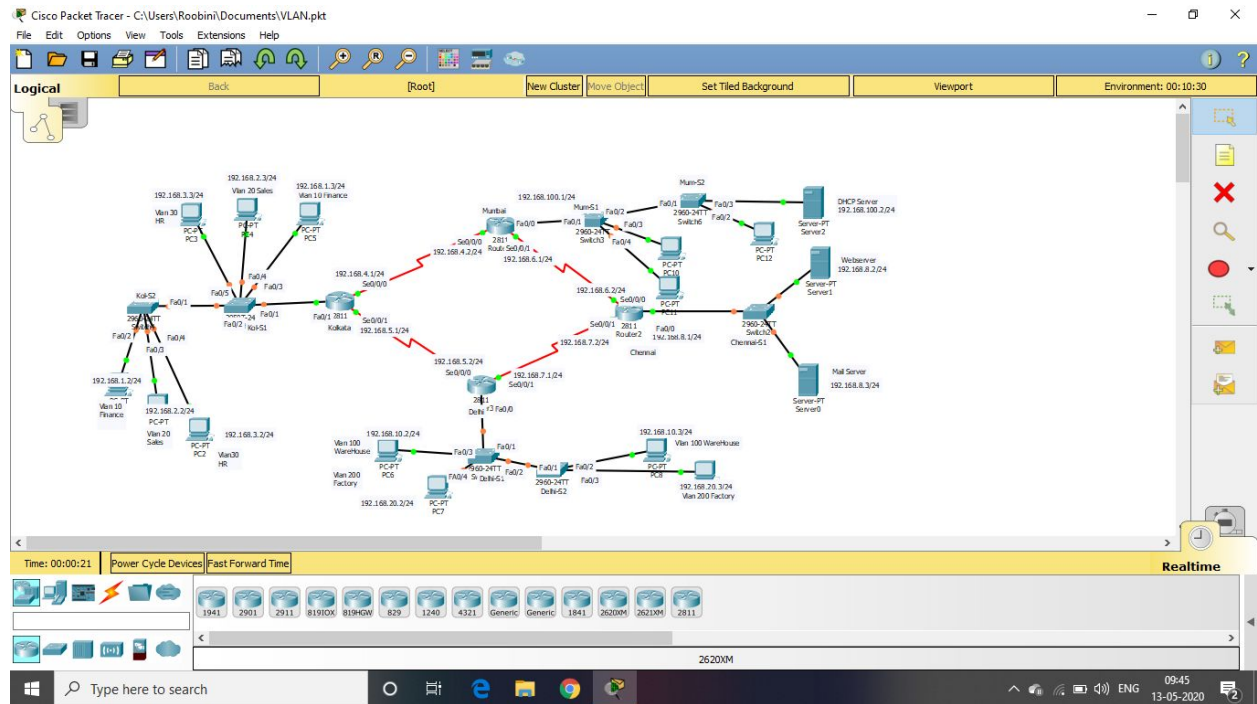


Figure 3: Main Network Simulation

Server2

Physical Config Services Desktop Programming Attributes

SERVICES

- HTTP
- DHCP
- DHCPv6
- TFTP
- DNS
- SYSLOG
- AAA
- NTP
- EMAIL
- FTP
- IoT
- VM Management

DHCP

Interface: FastEthernet0 Service: ☒ On ☐ Off

Pool Name: serverPool

Default Gateway: 192.168.100.1

DNS Server: 192.168.100.2

Start IP Address: 192.168.100.10

Subnet Mask: 255.255.255.0

Maximum Number of Users: 20

TFTP Server: 0.0.0.0

WLC Address: 0.0.0.0

Add Save Remove

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
serverPool	192.168.100.1	192.168.100.2	192.168.100.10	255.255.255.0	20	0.0.0.0	0.0.0.0

☐ Top

Figure 4: DHCP Server established

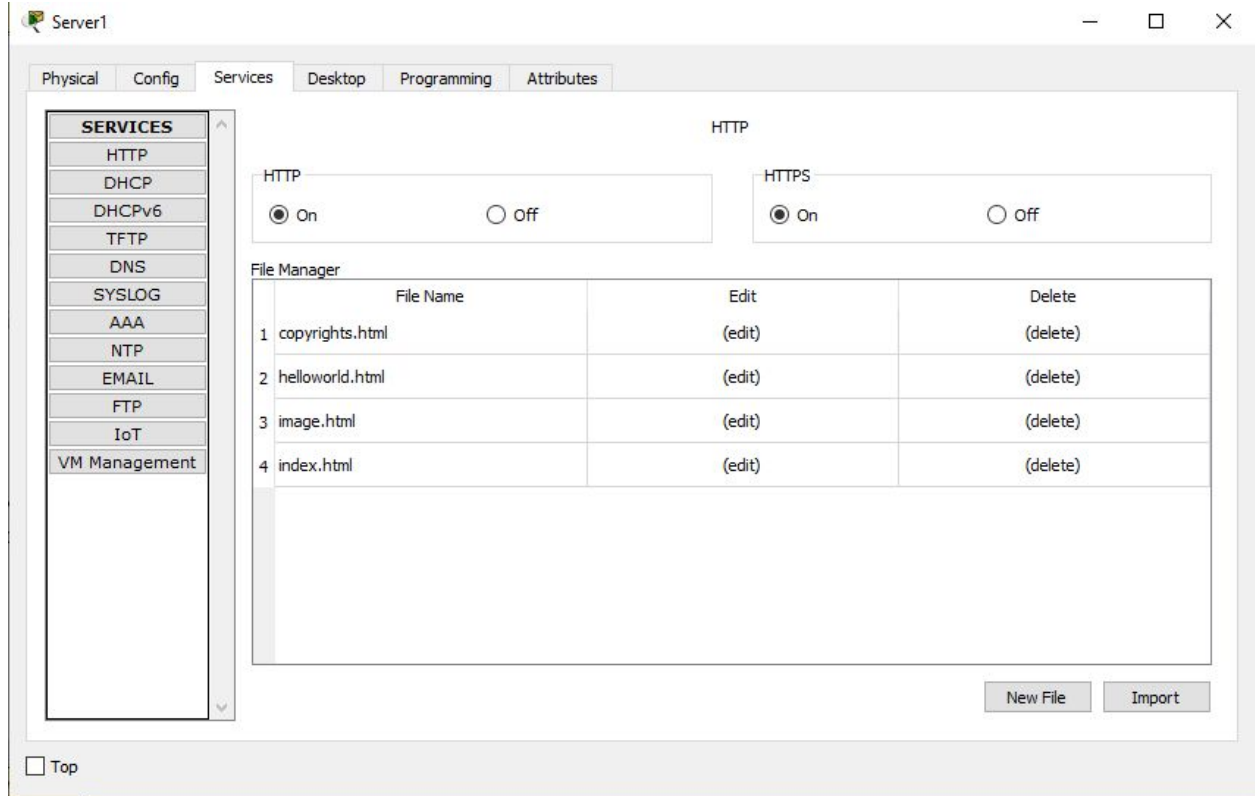


Figure 5: HTTP Server Established

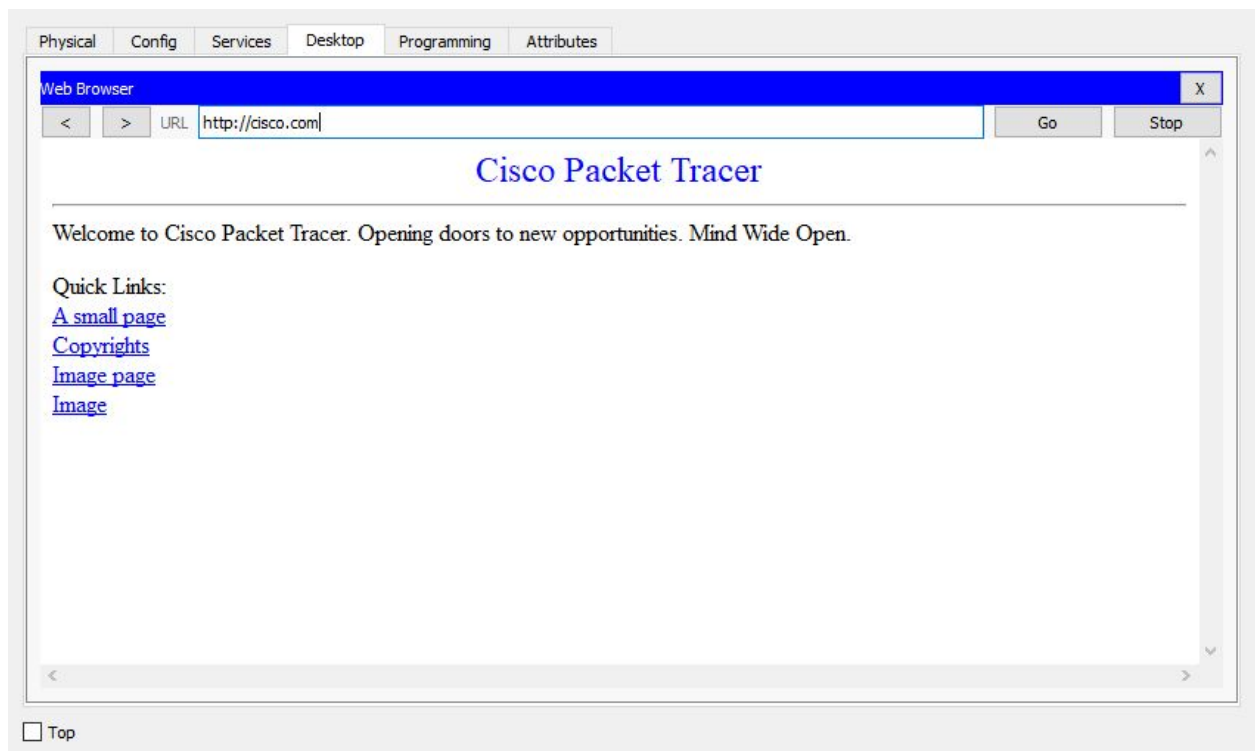


Figure 6: HTTP services enabled

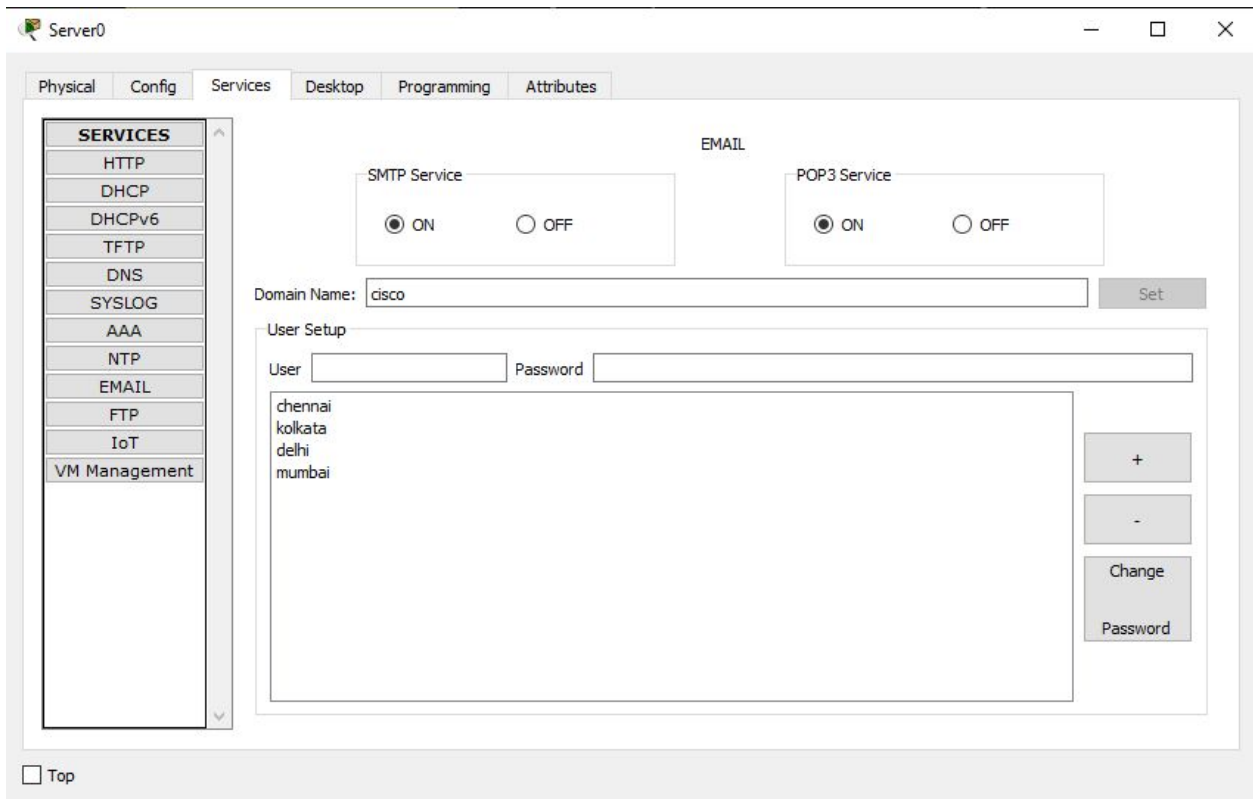


Figure 7: Mail Server established

Implementation: Github Repository: <https://github.com/vkmanojk/Networks-VirtualLAN>

VLAN:

A virtual LAN (VLAN) is any broadcast domain that is partitioned and isolated in a computer network at the data link layer (OSI layer 2). LAN is the abbreviation for local area network and in this context virtual refers to a physical object recreated and altered by additional logic. VLANs work by applying tags to network frames and handling these tags in networking systems – creating the appearance and functionality of network traffic that is physically on a single network but acts as if it is split between separate networks. In this way, VLANs can keep network applications separate despite being connected to the same physical network, and without requiring multiple sets of cabling and networking devices to be deployed.

VLANs allow network administrators to group hosts together even if the hosts are not directly connected to the same network switch. Because VLAN membership can be configured through software, this can greatly simplify network design and

deployment. Without VLANs, grouping hosts according to their resource needs the labor of relocating nodes or rewiring data links. VLANs allow networks and devices that must be kept separate to share the same physical cabling without interacting, improving simplicity, security, traffic management, or economy. For example, a VLAN could be used to separate traffic within a business due to users, and due to network administrators, or between types of traffic, so that users or low priority traffic cannot directly affect the rest of the network's functioning. Many Internet hosting services use VLANs to separate their customers' private zones from each other, allowing each customer's servers to be grouped together in a single network segment while being located anywhere in their data center. Some precautions are needed to prevent traffic "escaping" from a given VLAN, an exploit known as VLAN hopping.

To subdivide a network into VLANs, one configures network equipment. Simpler equipment can partition only per physical port (if at all), in which case each VLAN is connected with a dedicated network cable. More sophisticated devices can mark frames through VLAN tagging, so that a single interconnect (trunk) may be used to transport data for multiple VLANs. Since VLANs share bandwidth, a VLAN trunk can use link aggregation, quality-of-service prioritization, or both to route data efficiently.

VLAN Simulation Output and Verification:

```
Enter your telnet username: kelvin
Password:
Configuring SSH 192.168.122.72

SW1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)#ip domain-name nocturnalnetworking.com
SW1(config)#crypto key gen rsa
The name for the keys will be: SW1.nocturnalnetworking.com
Choose the size of the key modulus in the range of 360 to 4096 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 0 seconds)

SW1(config)#do wr
Building configuration...
Compressed configuration from 1672 bytes to 981 bytes[OK]
SW1(config)#end
SW1#exit

Configuring SSH 192.168.122.82

SW2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW2(config)#ip domain-name nocturnalnetworking.com
SW2(config)#crypto key gen rsa
The name for the keys will be: SW2.nocturnalnetworking.com
Choose the size of the key modulus in the range of 360 to 4096 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 0 seconds)

SW2(config)#do wr
Building configuration...
Compressed configuration from 1611 bytes to 931 bytes[OK]
SW2(config)#end
SW2#exit

Configuring SSH 192.168.122.83
```

Figure 8: VLAN simulation output

```
root@NetworkAutomation-1:~# ssh kelvin@192.168.122.82
The authenticity of host '192.168.122.82 (192.168.122.82)' can't be established.
RSA key fingerprint is SHA256:4eRnTT3wH0b5qzD7SDHJHK0nqmQFEVq7y+M66oYwB98.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.122.82' (RSA) to the list of known hosts.
Password:
SW2#
```

Figure 9: VLAN verification using SHA256

Routing Information Protocol (RIP):

The Routing Information Protocol (RIP) is one of the oldest distance-vector routing protocols which employ the hop count as a routing metric. RIP prevents routing loops by implementing a limit on the number of hops allowed in a path from source to destination. The largest number of hops allowed for RIP is 15, which limits the size of networks that RIP can support. RIP implements the split horizon, route poisoning and hold down mechanisms to prevent incorrect routing information from being propagated. In RIPv1 routers broadcast updates with their routing table every 30 seconds. In the early deployments, routing tables were small enough that the traffic was not significant. As networks grew in size, however, it became evident there could be a massive traffic burst every 30 seconds, even if the routers had been initialized at random times. In most networking environments, RIP is not the preferred choice for routing as its time to converge and scalability are poor compared to EIGRP, OSPF, or IS-IS. However, it is easy to configure, because RIP does not require any parameters, unlike other protocols.

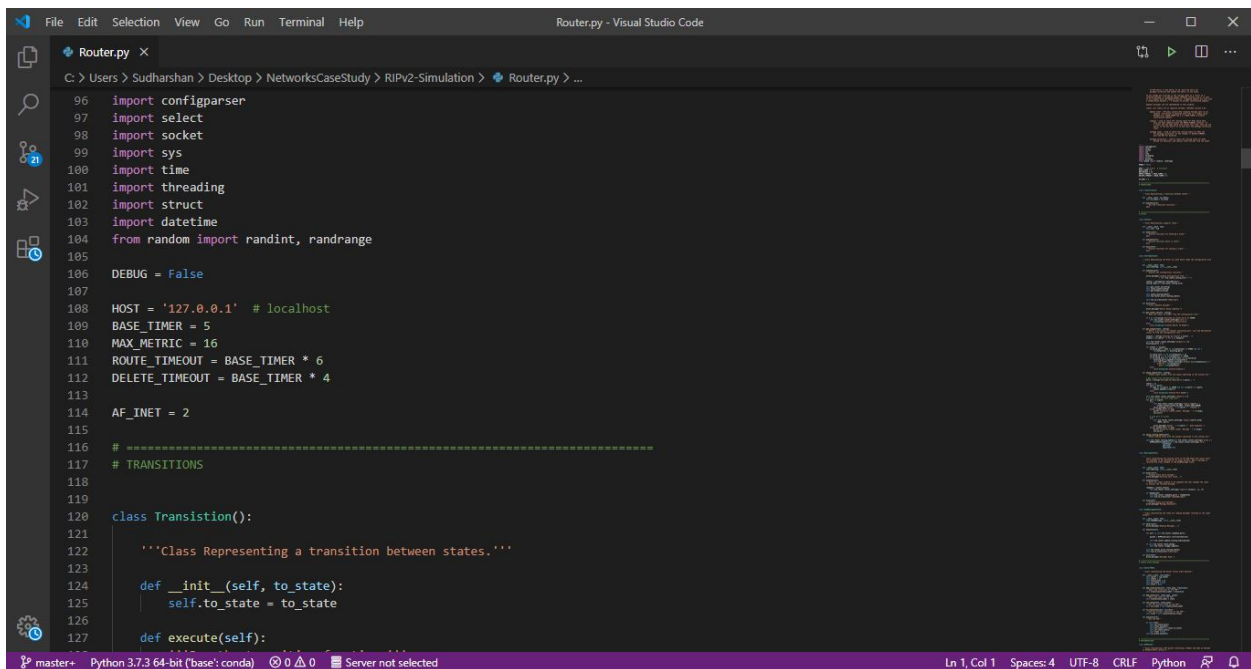
RIP uses the User Datagram Protocol (UDP) as its transport protocol, and is assigned the reserved port number 520.

RIP Version 2:

Due to the deficiencies of the original RIP specification, RIP version 2 (RIPv2) was developed in 1993, published as RFC 1723 in 1994, and declared Internet Standard 56 in 1998. It included the ability to carry subnet information, thus supporting Classless Inter-Domain Routing (CIDR). To maintain backward compatibility, the hop count limit of 15 remained. RIPv2 has facilities to fully interoperate with the earlier specification if all Must Be Zero protocol fields in the RIPv1 messages are properly specified. In addition, a compatibility switch feature allows fine-grained interoperability adjustments.

In an effort to avoid unnecessary load on hosts that do not participate in routing, RIPv2 multicasts the entire routing table to all adjacent routers at the address 224.0.0.9, as opposed to RIPv1 which uses broadcast. Unicast addressing is still allowed for special applications. (MD5) authentication for RIP was introduced in 1997. Route tags were also added in RIP version 2. This functionality allows a distinction between routes learned from the RIP protocol and routes learned from other protocols.

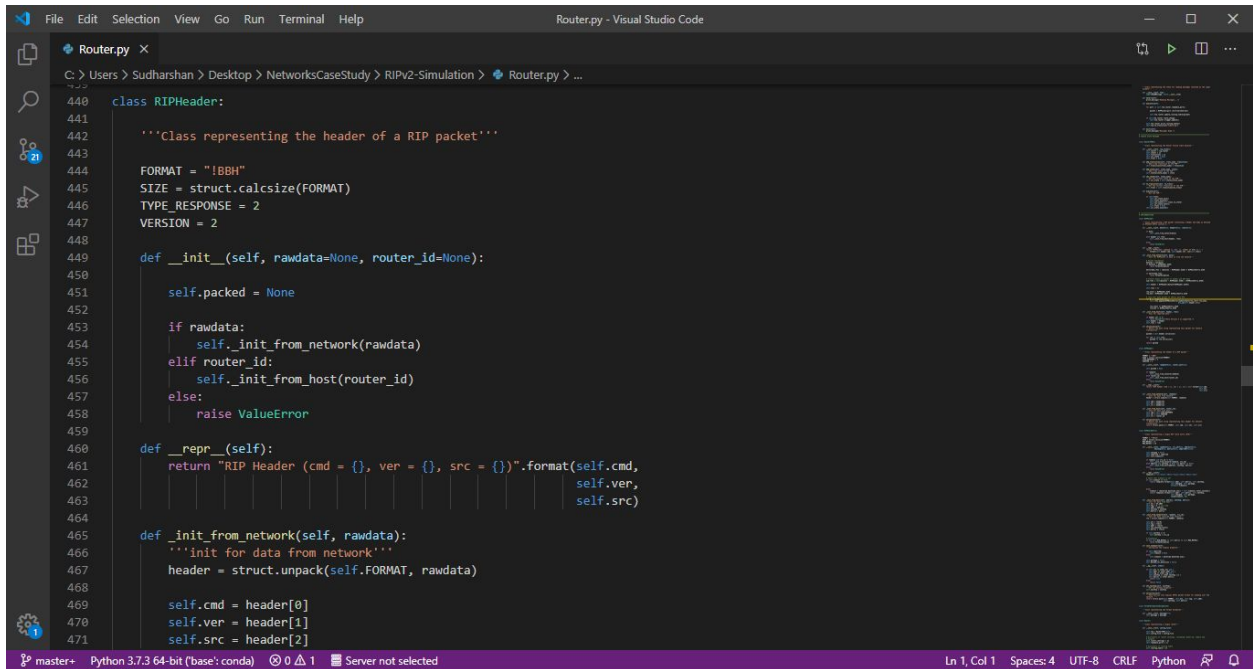
Screenshots:



```
Router.py
C:\Users\Sudharshan\Desktop> NetworksCaseStudy> RIPv2-Simulation> Router.py > ...

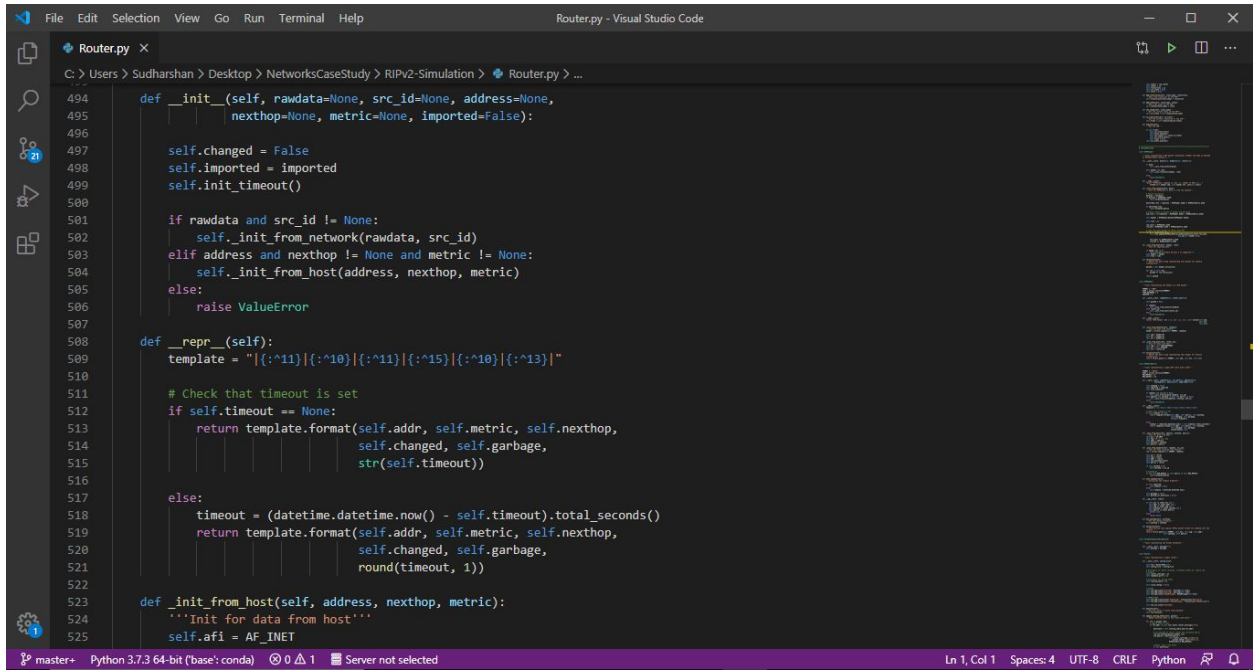
96 import configparser
97 import select
98 import socket
99 import sys
100 import time
101 import threading
102 import struct
103 import datetime
104 from random import randint, randrange
105
106 DEBUG = False
107
108 HOST = '127.0.0.1' # localhost
109 BASE_TIMER = 5
110 MAX_METRIC = 16
111 ROUTE_TIMEOUT = BASE_TIMER * 6
112 DELETE_TIMEOUT = BASE_TIMER * 4
113
114 AF_INET = 2
115
116 # =====
117 # TRANSITIONS
118
119
120 class Transition():
121     '''Class Representing a transition between states.'''
122
123     def __init__(self, to_state):
124         self.to_state = to_state
125
126     def execute(self):
127         ...
```

This shows the initial configurations of key parameters.



```
440 class RIPHeader:
441     '''Class representing the header of a RIP packet'''
442
443     FORMAT = "!BBH"
444     SIZE = struct.calcsize(FORMAT)
445     TYPE_RESPONSE = 2
446     VERSION = 2
447
448     def __init__(self, rawdata=None, router_id=None):
449         self.packed = None
450
451         if rawdata:
452             self._init_from_network(rawdata)
453         elif router_id:
454             self._init_from_host(router_id)
455         else:
456             raise ValueError
457
458     def __repr__(self):
459         return "RIP Header (cmd = {}, ver = {}, src = {})".format(self.cmd,
460                                                                    self.ver,
461                                                                    self.src)
462
463     def _init_from_network(self, rawdata):
464         '''init for data from network'''
465         header = struct.unpack(self.FORMAT, rawdata)
466
467         self.cmd = header[0]
468         self.ver = header[1]
469         self.src = header[2]
```

This shows the information about the RIP header. All the parameters it contains.



```
494 def __init__(self, rawdata=None, src_id=None, address=None,
495             nexthop=None, metric=None, imported=False):
496
497     self.changed = False
498     self.imported = imported
499     self.init_timeout()
500
501     if rawdata and src_id != None:
502         self._init_from_network(rawdata, src_id)
503     elif address and nexthop != None and metric != None:
504         self._init_from_host(address, nexthop, metric)
505     else:
506         raise ValueError
507
508     def __repr__(self):
509         template = "[{:^11}|{:~10}|{:~11}|{:~15}|{:~10}|{:~13}]"
510
511         # Check that timeout is set
512         if self.timeout == None:
513             return template.format(self.addr, self.metric, self.nexthop,
514                                    self.changed, self.garbage,
515                                    str(self.timeout))
516
517         else:
518             timeout = (datetime.datetime.now() - self.timeout).total_seconds()
519             return template.format(self.addr, self.metric, self.nexthop,
520                                    self.changed, self.garbage,
521                                    round(timeout, 1))
522
523     def _init_from_host(self, address, nexthop, metric):
524         '''Init for data from host'''
525         self.af = AF_INET
```

This shows the information about routing table entries. This contains details about what all details are inserted into the routing table.

IP Addressing:

VLAN IP :

- VLAN 10 (Finance) - 192.168.1.0/24
- VLAN 20(Sales) - 192.168.2.0/24
- VLAN 30 (HR) - 192.168.3.0/24
- VLAN 100 (WareHouse) - 192.168.10.0/24
- VLAN 200 (Factory) - 192.168.20.0/24

LAN IP :

- Chennai LAN - 192.168.8.0/24
- Mumbai LAN - 192.168.100.0/24

WAN IP:

- Kolkata to Delhi WAN - 192.168.5.0/24
- Kolkata to Mumbai WAN - 192.168.4.0/24
- Chennai to Mumbai WAN - 192.168.6.0/24
- Chennai to Delhi WAN - 192.168.7.0/24

Sufficiency of the Network:

1. *Network Security:* Whenever a station transmits in a shared network such as a legacy half-duplex 10BaseT system, all stations attached to the segment receive a copy of the frame, even if they are not the intended recipient. If the users on the network belong to the same department, this might not be disastrous, but when users from mixed departments share a segment, undesirable information captures can occur. However, in the proposed network design, when a station transmits, the frame goes to the intended destination.
2. *Bandwidth Utilization:* When users attach to the same shared segment, they share the bandwidth of the segment. The more users that attach to the shared cable means less average bandwidth for each user. VLANs, which are usually created with LAN switch equipment, can offer more bandwidth to users than is inherent in a shared network.

3. *Network Latency from Routers:* As a frame passes through a router, the router introduces latency—the amount of time necessary to transport a frame. Every router that the frame transits increases the end-to-end latency. Further, every congested segment that a frame must cross increases latency. By moving all of the users belonging to the same department into one VLAN, the need to cross through multiple routers and segments is eliminated.
4. *Complex Access Lists:* Through the implementation of access lists, you can prevent a specific user from communicating with another user or network, or you can prevent an entire network from accessing a user or network. VLANs can help by allowing you to keep all users in a specific department in one VLAN. Then their traffic does not need to pass through a router to get to peers of the VLAN. This can simplify your access list design because you can treat networks as groups with similar or equal access requirements.
5. *Routing:* The Routing Information Protocol version 2, uses dynamic programming to calculate the minimum distance between two nodes, hence providing an efficient way to reduce congestion.

QoS Parameters:

Bandwidth: Bandwidth is the capacity of a wired or wireless network communications link to transmit the maximum amount of data from one point to another over a computer network or internet connection in a given amount of time. Expressed in bits per second (bps), modern network links have greater capacity, which is typically measured in millions of bits per second (megabits per second, or Mbps) or billions of bits per second (gigabits per second, or Gbps). Bandwidth of the proposed design is 10,000 Kbits/sec

Throughput: Throughput measures the percentage of data packets that are successfully being sent; a low throughput means there are a lot of failed or dropped packets that need to be sent again.

$$\text{Throughput} = \frac{\sum(\text{no. of packets} * \text{avg packet size})}{\text{Total time spent in delivering the data}} ; \text{throughput of Cisco 2811 is 61 Mbps}$$

Packet Loss: Packet loss occurs when one or more packets of data travelling across a computer network fail to reach their destination. Due to network congestion.

Number of packets sent = 5

Successfully transmitted packets = 4

Efficiency = $100\% * (\text{transferred} - \text{retransmitted}) / \text{transferred}$
= $100 * (5 - 1) / 5 = 80\%$

Network loss = $100 - \text{Efficiency} = 20\%$

```
Mumbai>ping 192.168.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2
seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/4
ms

Mumbai>|
```

Transmission time: The time required for transmission of a message depends on the size of the message and the bandwidth of the channel.

$$\text{Transmission time} = \frac{\text{Message Size}}{\text{Bandwidth}} = \frac{100 \text{ bytes}}{10000 \text{ Kbps}} = 80\mu\text{s}$$

Propagation Delay: Propagation time measures the time required for a bit to travel from the source to the destination. The propagation time is calculated by dividing the distance by the propagation speed.

$$\text{Propagation time} = \frac{\text{Distance}}{\text{Propagation Speed}} = 100\mu\text{s}$$

Processing Delay: Time taken by the processor to process the data packet is called processing delay. Processing Delay is directly proportional to the processing speed of the processor.

Queuing Delay: Time spent by the data packet waiting in the queue before it is taken for execution is called queuing delay. Queuing Delay is directly proportional to the congestion in the network.

Network Latency: Network latency is the time it takes for data or a request to go from the source to the destination. Latency in networks is measured in milliseconds. The closer your latency is to zero, the better.

$$\begin{aligned} \text{Network Latency} &= N * (N^{th} (D_{prop}) + N^{th} (D_{trans})) \\ &= 540 \mu s \end{aligned}$$

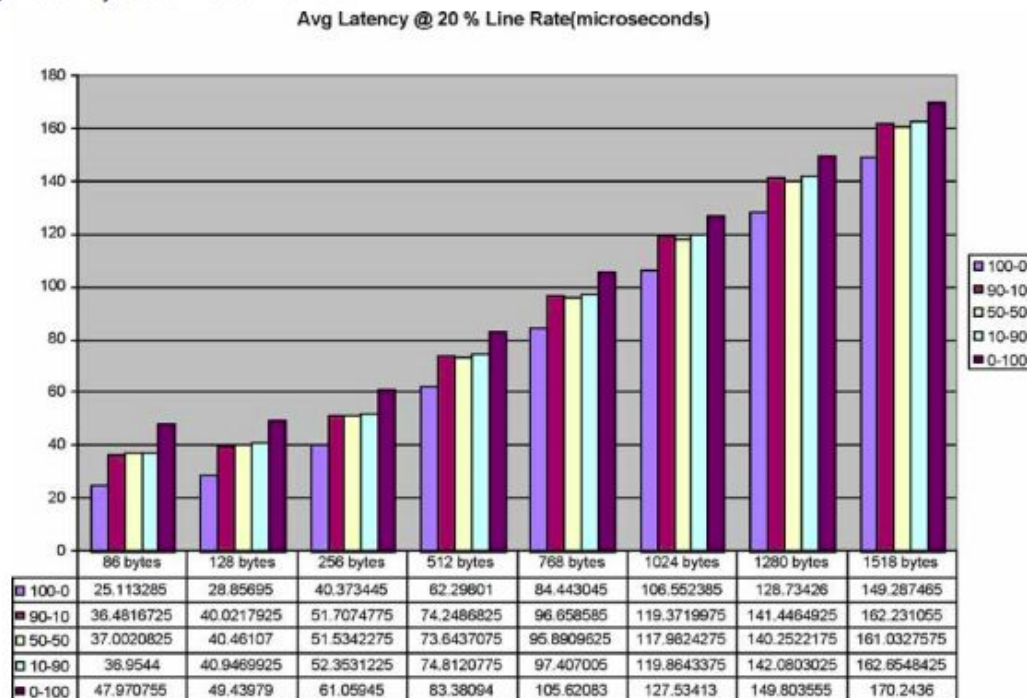
where,

N is the number of intermediate nodes

D_{prop} is the propagation delay

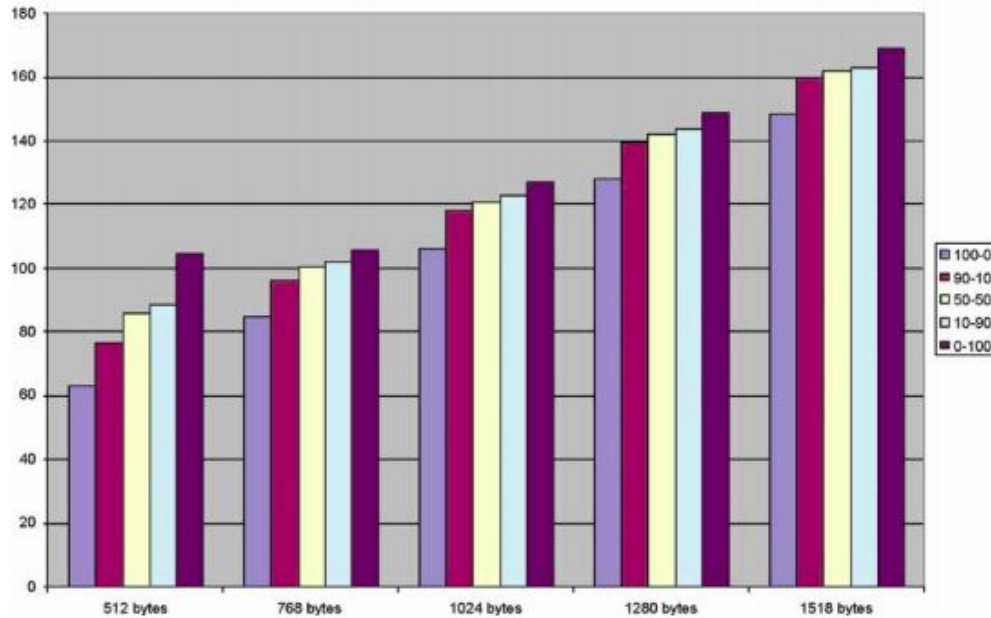
D_{trans} is the transmission delay

Average Latency at the 20% Line Rate



Average Latency at the 90% Line Rate

Avg Latency @ 90 % Line Rate(microseconds)



Conclusion:

In conclusion, a prototype network was designed and implemented in this research work using the Cisco Packet Tracer software. Our objective was to design and simulate an efficient VoIP network scenario for the case study and also to configure the virtual network devices of the simulation, evaluating point-to-point connections to ensure proper communication between various offices and departments. To implement this, we had to study the whole VLAN scenario, its features, benefits, drawbacks and its future in the networking world. Overall, this study improved our understanding of the whole concept of VLAN and its ever increasing demand in present times. As a result of this work, the solution implemented can be modified according to any organization's requirements. The effective implementation of VLAN enhances the network security by keeping devices that operate with sensitive information on a separate VLAN. This is especially useful, because the workstations can be easily relocated if and when necessary. The key element to the Inter-VLAN routing service is that there must be at least one VLAN interface configured with an IP Address on the Inter-VLAN capable switch.

References:

- Andrew S. Tanenbaum, Computer Networks, Prentice Hall, Fourth Edition, 2002.
- C. Archana, “Analysis of RIPv2, OSPF, EIGRP Configuration on router Using CISCO Packet tracer,” International Journal of Engineering Science and Innovative Technology, vol. 4, Issue 2, pp. 2015.
- S. S. Tambe, “Understanding Virtual Local Area Networks,” International Journal of Engineering Trends and Technology, vol. 25, no. 4, 2015.
- <http://www.firewall.cx/networking-topics/vlan-networks/222-intervlan-routing.html>
- <http://searchnetworking.techtarget.com/tutorial/VLAN-guide-for-networking-professionals>
- https://en.wikipedia.org/wiki/Virtual_LAN
- G. Thrivikram, “Implementation of Virtual LAN (VLAN) using Layer3 Switches,” International Journal of Advance Research in Computer Science and Management Studies, vol. 4, Issue 3